Digital Security — A Question of Perspective
A Large-Scale Telephone Survey with Four At-Risk User Groups

Franziska Herbert*, Steffen Becker*†, Annalina Buckmann*, Marvin Kowalewski*,
Jonas Hielscher*, Yasemin Acar‡, Markus Dürmuth§, Yixin Zou†, and M. Angela Sasse*
*Ruhr University Bochum, Germany †Max Planck Institute for Security and Privacy, Germany
‡Paderborn University, Germany §Hannover University, Germany
Email: {franziska.herbert, steffen.becker, annalina.buckmann, marvin.kowalewski, jonas.hielscher, angela.sasse}@rub.de,
yasemin.acar@uni-paderborn.de, markus.duermuth@itsec.uni-hannover.de, yixin.zou@mpi-sp.org

***Abstract*—This paper investigates the digital security experiences of four at-risk user groups in Germany, including older adults (70+), teenagers (14-17), people with migration backgrounds, and people with low formal education. Using computer-assisted telephone interviews, we sampled 250 participants per group, representative of region, gender, and partly age distributions. We examine their device usage, concerns, prior negative incidents, perceptions of potential attackers, and information sources. Our study provides the first quantitative and nationally representative insights into the digital security experiences of these four at-risk groups in Germany. Our findings show that participants with migration backgrounds used the most devices, sought more security information, and reported more experiences with cybercrime incidents than other groups. Older adults used the fewest devices and were least affected by cybercrimes. All groups relied on friends and family and online news as their primary sources of security information, with little concern about their social circles being potential attackers. We highlight the nuanced differences between the four at-risk groups and compare them to the broader German population when possible. We conclude by presenting recommendations for education, policy, and future research aimed at addressing the digital security needs of these at-risk user groups.**

1. Introduction

Recent advancements in usable security and privacy research have challenged the notion of a "general user" [1], [2], argued to acknowledge user diversity [3], and shown the specific threat models, risks, and needs of various at-risk groups [4], [5], [6], [7] – individuals and communities with "risk factors that augment or amplify their chances of being digitally attacked and/or suffering disproportionate harms" [8]. At-risk populations generally face disproportionate challenges in protecting their security and privacy due to disparities in digital literacy, resources, time, and linguistic and cultural barriers [4], [8]. Including at-risk groups in research helps generate insights on their unique risks and needs, and inform more inclusive design of technologies and educational materials.

While there has been a growing body of research on at-risk groups, such research is predominantly qualitative [4] and conducted with small and specific groups, such as the LQBTQ+-community [9], [10], [11], undocumented migrants or refugees [12], [13], [14], and survivors of intimate partner abuse [15], [16], [17], [18], leading to valuable population-specific findings. Warford et al. took the first step of synthesizing contextual risk factors across different at-risk populations, emphasizing societal factors (e. g., legal or political), relationships (e. g., reliance on a third party), and personal circumstances (e. g., constrained resources, lack of accessibility) [8]. However, to our knowledge, there has not been any large-scale study with representative samples for these groups, which enables quantitative comparisons to identify the similarities and differences between multiple at-risk groups regarding their security experiences.[1]

Our study makes the first step to addressing this gap with a large-scale computer-assisted telephone interview (CATI) study with 1003 participants in total from four at-risk groups in Germany: older adults (70+), teenagers (14-17),[2] people with migration backgrounds,[3] and people with little formal education (less than high school).[4] Past literature has characterized the four groups as at-risk groups due to various reasons, e. g., teenagers are especially at risk of experiencing cyberbullying [21] and older adults are especially at risk of being targeted for tech scams and romance fraud [22]. The four groups also have varying degrees of representation in existing usable security and privacy literature, e. g., there is much more related work on older adults than on people with low formal education, but all groups have been less

1. We use the term "security experiences" to refer to participants' device usage, security and privacy concerns, previous negative security- and privacy-related incidents, perceptions of potential attackers, and security information sources. The topics represent core elements of participants' digital security experiences and relevant context.

2. For participating in a survey in Germany, the ability to consent is crucial. As German law views teenagers from 14 years onward as criminally responsible (see §19 StGB, §§1 Abs. II, 3 JGG) consent ability is assumed.

3. "Migration backgrounds" is a specific category mostly used in German-speaking countries, referring to residents who either have at least one parent who was born outside of Germany, who themselves migrated to Germany, and/or who hold a foreign citizenship [19].

4. International Standard Classification of Education (ISCED) 0-2 [20]

represented in large-scale quantitative studies [23], [24]. We focus on these four groups considering the quantitative nature of our research, as each group is broad enough to gather a nationally representative sample of each groups' population in terms of gender, region, and partly age.

Our telephone survey collected participants' responses on the following topics: device usage, concerns, prior negative incidents, perceptions of potential attackers, and information sources. Knowing which devices are being used helps contextualize the risks each group might encounter. Eliciting their security concerns, potential attackers, and prior negative incidents helps understand the specific threat landscape for each population. The experience of threats and concerns may motivate information-seeking behavior, and identifying the information channels they consult (or not) informs how to target each groups.

Our research is guided by the following questions:

RQ1: What are the security experiences (device usage, concerns, prior negative incidents, perceptions of potential attackers, information sources) for older adults, teenagers, people with migration backgrounds, and people with low formal education?

RQ2: How similar or different are the four groups in terms of their security experiences?

Summary of key findings. Participants with migration backgrounds stand out for using the most devices, seeking more security information than the other groups, but also reporting most experiences with cybercrime incidents. In contrast, older adults used the fewest devices and were least affected by cybercrime. Participants shared diverse concerns about digital security and there was no predominant concern across all groups. In terms of similarities, many participants across the groups reported being affected by malware and turning to their inner social circle (i. e., family and friends) for information on digital security, without considering them as potential attackers. We compare our findings to prior (mostly qualitative) work and the broader German population when possible. For example, we find that our participants encountered cybercrime incidents much more frequently than the average German population [25], providing empirical evidence that these groups are indeed at higher risks of cybercrime and underscoring the need to protect these groups through better educational efforts and public policy.

2. Group-Specific Prior Research

We summarize the key findings of related work regarding the four at-risk groups. While our four sample groups tend to be underrepresented in quantitative security and privacy research [23], [24], several (mostly qualitative) studies have investigated these at-risk groups.

2.1. Older Adults

There has been a considerable body of qualitative research on older adults' perceptions of privacy and security, both broadly [26], [27], [28] and with regard to specific contexts such as social media [29], [30] and healthcare [31], [32]. For example, Frik et al. 's study highlights older adults' differing attitudes toward privacy versus security, misconceptions about data flows, and blind spots in mitigation strategies, making them limit or avoid technology use altogether [26].

Similarly, Ray et al. 's study shows how the perceived vulnerability of private information leaves many older adults anxious or frustrated, causing them to shy away from using online services [28]. Older adults also have particular needs that have not been sufficiently considered in mainstream security and privacy mechanisms. For example, older adults may find it challenging to manage passwords due to memory difficulties [27], [33], and because of that the management is often delegated to friends or family members.

Regarding advice sources, older adults were found to value social resources over expert advice, and they avoid using the Internet for cybersecurity information despite using it for other topics [34].

2.2. Teenagers

Teenagers tend to be digital natives as they are increasingly using digital technology from an early age [35]. The easy and nearly constant access to the internet comes with risks, not only for typical cybersecurity incidents (e. g., phishing, hacking, and identity theft) [21] but also for events that can threaten one's psychological or even physical safety (e. g., exposure to unwanted explicit content, harassment, and sexual solicitations) [36].

Prior work has found that teens "make online disclosures and render themselves more susceptible to experiences of risky online interactions"; which in turn generate privacy concerns, advice-seeking, and risk-coping behaviors [37]. Resilience is not only a key factor protecting teens from experiencing online risks, but also neutralizes negative psychological effects associated with Internet addiction and online risk exposure [38]. In terms of information sources, teenagers often turn to peers and online platforms to seek support on topics like online sexual interactions [39], but are more reserved in discussing risky experiences with parents [40]. Also, parent involvement through control (i. e., control apps) was associated with increased risks [41].

2.3. Migration Backgrounds

There have been multiple studies about the digital experiences of people with migration backgrounds especially refugees [13], [14], [42], [43], [44], [45], [46], [47], [48], [12]. Guberek et al.'s study with undocumented immigrants in the United States identifies key concerns about identity theft, privacy, and online harassment, but participants' concerns about government surveillance are vague and intertwined with resignation [12]. Similarly, Simko et al.'s study with refugees shows how reliance on technology (e. g., for finding jobs and establishing a life) forces security "best practices" into the background [13]. Focusing on people who

recently migrated to Germany, Stapf [44] found that they are familiar with concepts of misinformation and hate speech on social media, but also value social media for information seeking and counseling; meanwhile, information from official sources and websites is perceived as inaccessible, hard to understand, and not always helpful compared to information shared in their own language or based on other's personal experiences.

2.4. Low Formal Education

There is less related work on people with little formal education compared to other groups, and most related work we find for this group has been conducted in the US context. Among research on education and its effect on one's security and privacy experiences, it has been found that individuals with lower education tend to be less concerned about online privacy issues [49] and doubt their Internet service providers' ability to protect their personal information [50], whereas those more educated are more likely to utilize privacy protection measures [51], such as reading privacy policies [52], [53]. Bergström's study highlights the particular concerns held by people with lower education regarding information search, email handling, and using debit cards [54]. On the topic of viruses and hackers, Wash and Rader's study suggests that internet users with less education are more likely to show resignation; those with higher education report taking more protective actions but also rarely consider themselves to be vulnerable [55].

Other studies have used lower socioeconomic status (SES) as a proxy for lower education. A Pew 2017 survey highlights a knowledge gap on issues around privacy and security, as respondents with lower education scored lower in a 13-item quiz [56]. On the contrary, Redmiles et al.'s study finds that people's reported experiences of negative incidents are significantly related to advice sources, regardless of their SES or resources [57].

3. Research Method

To draw representative samples for the four at-risk groups, we employed computer-assisted telephone interviews (CATIs). We chose CATIs for several reasons. (1) CATIs allow for misunderstandings to be clarified as participants have the opportunity to ask questions. (2) Compared with computer-assisted personal interviews (CAPIs), which also allow clarifying questions, CATIs are less expensive, and more participants can be interviewed in less time [58], [59]. (3) For open-ended questions, participants are likely to provide more information in CATIs than in online surveys as they do not have to type out their answers, which also helps increase data quality. (4) CATIs enable us to collect both qualitative and quantitative data, which can provide complementary insights. (5) CATIs are generally considered a high-quality data collection method compared to paper and pencil surveys [58].

CATIs also offer particular advantages for recruiting our target populations. Almost every household in Germany can be reached by telephone,[5] so the majority of the population – including our four groups – can be reached. Unlike online surveys, CATI participants do not need to be highly computer literate – this is an important factor to consider as our target groups include older adults and people with low levels of formal education [58]. In fact, prior work has recommended using telephone surveys to reach populations such as older adults [59]. Our data collection also took place during the COVID-19 pandemic, which made in-person interviews difficult and CATIs a better alternative.

3.1. Questionnaire

Our CATI questionnaire contains fourteen closed questions and one open-ended question. We pilot-tested the questionnaire in multiple rounds to verify that the duration is manageable and the questions are understandable over the phone. Below we provide an overview of all questions used for this work. The entire questionnaire can be found in Appendix A.

3.1.1. Introduction and Informed Consent. Before starting with the actual questionnaire, interviewers introduced themselves, briefly stated the aim of the research and the planned duration of the interview. Participants were informed that they could terminate the interview at any time, that the telephone interview would not cause any harm, and that they could choose not to respond to any question. We only interviewed participants after they provided informed consent.

3.1.2. Demographics and Technology Usage. The first five questions were demographic screening questions to filter participants for the desired target groups with the intended representativeness criteria. If interviewees did not fit any of the at-risk groups, the interviewer politely ended the interview. If interviewees were eligible, the interview began with a question about the device types they use in their daily lives (Q1). We included the question since device usage may influence one's exposure to corresponding threats. For example, mobile devices face particular threats related to location tracking [61], [62], [63]. There are also particular vulnerabilities for IoT devices, such as weak voice authentication [64] and continuous listening and recording [65].

3.1.3. Concerns, Prior Incidents, Advice Sources, and Potential Attackers. Our next questions queried participants' concerns and prior experience with digital security threats. These questions help generate insights and implications for how to eliminate unnecessary fears and misconceptions among our participants and provide them with relevant information on protective strategies.

To avoid priming, this segment started with an open-ended question eliciting participants' concerns about their digital security (Q4). In a follow-up question, participants

5. In 2022, 99.9% of German households were equipped with either a landline or cell phone [60].

were asked whether they had already experienced various types of cybercrime identified in a survey by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik; BSI) [66], such as malware, phishing and cyberbullying (Q6). We then asked participants if and where they seek information about digital security (Q7 and Q8) to identify the channels best used to reach each group.

To elicit participants' threat models and identify possible blind spots, we provided participants with eight groups of potential attackers (e. g., family members or officials from Germany) and asked them to rate how likely each group might pose a risk to their digital security (e. g., by obtaining unauthorized access to their personal data, stalking them online, or restricting their access to digital services) (Q10). Response options consisted of a five-point rating scale ranging from *1–not likely* to *5–very likely*.

3.2. CATI Implementation and Panels

Interviews were conducted between October and December 2021 by professional telephone interviewers.

Phone number sampling was based on a master sample, which contained up-to-date information on the range of numbers available in the German telephone network, with a distribution of 70% landline numbers and 30% mobile numbers generated at random [67], [68]. Prior to data collection, we conducted a training session with the interviewers, explaining the purpose of the study and guiding them step-by-step through the questionnaire, thereby giving them the opportunity to ask questions. Additionally, we supplied the interviewers with a glossary to prepare them for any potential questions from participants. During the interview, the interviewers introduced themselves on behalf of our institution. If the invitee agreed to participate, their responses were recorded by interviewers using a web interface. The telephone interviews were conducted on multiple days of the week and at several times of the day. Participants who terminated the interview early or withdrew consent to analyze their data were excluded from the final data set. We cannot make any statements about the response rates because the CATI provider did not disclose them to us.

For each of the four groups, about 250 participants were interviewed, resulting in a total of 1003 telephone interviews (see Table 1 for further demographic details on each group). All four groups were sampled to be representative of their respective gender and regional distribution in Germany [69], [70]. The groups with low formal education and migration backgrounds were each sampled to be group-representative in terms of age as well. For example, the quota for participants with migration backgrounds aged 35 to 54 was 95 participants. Our samples matched the target quotas with only small discrepancies ranging from 1% to 4% with the exception of gender quotas for teenagers and older adults, which were met with 8 respectively 9% deviation. As common with CATIs, participants were not compensated.

6. Many participants in this group had not yet graduated from school.

There are natural overlaps between the four groups as a result of our sampling strategy (e.g., some older participants in the older adults group may also have migration backgrounds and/or low levels of formal education). These overlaps reflect the representative composition of these groups in Germany and allow us to display the diversity of these groups as it exists.

3.3. Data Analysis and Coding Procedure

All data was first analyzed descriptively, except for the open-ended question (Q4). We then performed X^2 tests for all differences greater than 5% to determine which groups differ significantly regarding binary data (Q1, Q6, Q7). We used Bonfferoni-Holm alpha correction to account for multiple testing. To identify significant differences between the groups for interval data (Q9), we used (Welch-)ANOVAs with Bonferroni corrected post-hoc tests. Regarding effect sizes, we report phi for X^2 tests and *Cohen's d* for the ANOVA post-hoc tests [71].

For analyzing text responses (Q4), we used qualitative content analysis [72]. Three researchers coded the first 150 responses independently, compared their codes, and agreed upon an initial codebook. Subsequently, the same three researchers coded the remaining responses independently. We calculated Fleiss' Kappa to determine inter-rater reliability (IRR), which was considered moderately acceptable ($\kappa = 0.74$) [73]. Finally, the three researchers jointly reviewed unclear cases and summarized the codes under broader categories. We provide the complete codebook and code distributions for each group in Appendix B.

3.4. Positionality Statement

As researchers, we are aware that our own backgrounds, values, and biases influence how we conduct research [74] and we are always at risk of reproducing knowledge that reifies power [75]. We strive to accurately represent the perspectives of the groups we study while critically reflecting on our approach. Our team comprises highly-educated researchers from the disciplines of psychology, usable security and privacy, and security engineering. None of us belong to the groups of teenagers, older adults, or people with lower formal education. We acknowledge that our relative privilege within society (particularly high education) provides us with certain advantages that our participants do not hold. However, two members have conducted research with older adults in the past, and two members have migration backgrounds themselves, which gives us relevant insights into these groups.

3.5. Ethics

As our department does not have an institutional review board, we had extensive ethics-related discussions within our interdisciplinary team. We also developed a protocol that followed best practices of human subjects

Table 1. DEMOGRAPHICS AND DEVICE USAGE OF THE FOUR AT-RISK GROUPS.

		Older Adults n=250		**Teenagers** n=250		**Migra. Backgr.** n=251		**Low Education** n=252	
		n	%	n	%	n	%	n	%
Age	14-17	0	0	250	100	0	0	0	0
	17-35	0	0	0	0	103	41	39	15
	36-50	0	0	0	0	63	25	48	19
	51-65	0	0	0	0	57	23	68	27
	66-69	0	0	0	0	14	5	75	30
	70+	250	100	0	0	14	5	22	9
Gender	Male	130	52	111	44	128	49	128	51
	Female	120	48	138	55	123	51	124	49
	Non-binary	0	0	1	1	0	0	0	0
Region	North	39	16	42	17	37	15	38	15
	East	45	18	51	20	28	11	24	10
	South	76	30	70	28	82	33	86	34
	West	90	36	87	35	104	41	104	41
Education	Low (ISCED 0-2)	126	50	31	13	50	20	252	100
	Medium (ISCED 3-4)	57	22	63	25	103	41	0	0
	High (ISCED 4-8)	56	22	0	0	96	38	0	0
	Other	11	4	156[6]	62	3	1	0	0
Device Usage	Smartphone	185	74	249	99	244	97	229	91
	Laptop or Desktop PC	194	78	207	83	222	88	215	85
	Tablet	88	35	138	55	144	57	121	48
	Smart Speaker	23	9	54	21	72	29	46	18
	Wearables	28	11	64	26	96	38	64	25
	None	12	5	18	7	13	5	17	7

research [76] and data protection guidelines, including the European General Data Protection Regulation (GDPR). All data protection measures were reviewed and approved by our institution's data protection office. Additionally, the CATI provider signed an agreement with our institution to follow GDPR guidelines. We ensured accessible language to not overwhelm participants or leave them frightened after the interview. We also followed current German law allowing teenagers of 14 years and above to take part in surveys without their parents' consent. The CATI research method and our provider did not allow us to compensate our participants financially or to provide them with information on digital security. However, we hope our publications will provide useful insights for our target groups so they may benefit in the long run.

3.6. Limitations

First, our study was conducted with German residents only, and our findings might not generalize to other countries or societies. Second, some questions required participants to admit gaps in their knowledge or mistakes they may have made – something they may be less likely to answer truthfully compared to neutral questions [23]. We tried to overcome this limitation through careful questionnaire design and by letting participants know that there are no wrong answers and they would not be judged. Third, to avoid bias, especially for the open-ended question (Q4), we decided against randomizing the question order. We thus can not preclude response order effects. Fourth, there are other at-risk groups that should be represented in research [2]; for example, our provider did not offer the possibility to interview participants that are differently abled or children under 14. Fifth, some of the related work referenced throughout the paper was performed before the COVID-19 pandemic. As the global population [77] as well as specific groups such as older adults [78] experience changes in Internet usage during the pandemic, this has implications for their security experiences and needs to be considered when comparing our findings with previous studies. Finally, based on our research design, we can only describe group-level differences but cannot accurately identify specific reasons that explain these differences.

4. Results

Our results section is organized as follows: First, we present findings on device usage, before we move on to participants' concerns regarding their digital security and their past experiences with cybercrime. Finally, we report our findings on participants' perceptions of potential attackers and end with the results on the sources of information they use most frequently.

4.1. Device Usage

Table 1 shows an overview of used devices per group: Overall, all groups reported high use of smartphones and PCs, followed by tablets; IoT devices such as smart speakers and wearables were used less frequently. Only 5 to 7

percent of each user group do not use any of the devices queried, i. e., the use of at least one Internet-enabled device is consistently high in all groups. The average number of used device types is 3.0 for teenagers, 2.3 for older adults, 3.4 for participants with migration backgrounds, and 3.0 for participants with low formal education. Comparing our findings to the Germany-wide BSI survey [25], our participants' usage rates are higher for smartphones (89%) and Laptops (71%) but more similar to the German public for tablets (53%) and wearables (22%).

In terms of between-group differences, older adults had significantly lower device usage overall: their smartphone and wearable usage is significantly lower than that of the other three groups; they also use tablets and smart speakers less often than teenagers and participants with migration backgrounds. In addition, people with low formal education reported significantly less prevalent smartphone usage than teenagers and people with migration backgrounds. Participants with a migration backgrounds reported significantly higher rates of wearable use compared to the other groups. Effect sizes for significant differences range between small (0.13) and moderate (0.38).

Summary. Participants with migration backgrounds are the most active users of Internet-enabled devices, while older participants use them least commonly. Teenagers and participants with low formal education are in the middle of the spectrum and show relatively small differences between each other.

4.2. Digital Security Concerns

For the open question asking for participants' concerns regarding their digital security (Q4), the response rates are higher for people with migration backgrounds (49%) and low formal education (49%). In contrast, 38% of teenagers and 34% of older adults stated any digital security concerns. 12 participants across all groups explicitly stated that they had no concerns (e. g., *"I am not really concerned, because you have protections you can rely on. I make sure that I have the latest programs."*).

The shared concerns varied significantly across all groups; no specific concern was raised by a majority of participants. This finding indicates that there is a wide diffusion of scattered risk awareness among these groups rather than a solidified "body of knowledge." It could also be a reflection of users being overwhelmed by the large body of security advice that lacks prioritization [79], [80].

We next present the more salient and prevalent concerns in Table 2 (including example quotes translated from German). The percentages stated in the following are based on only those who stated any concerns rather than all participants.

Hacking. Attacks by "hackers" were one of the concerns named across all groups – teenagers were slightly more concerned (24%) than participants with migration backgrounds and those with low education (both 19%), older adults were slightly less concerned (16%). One participant with migration backgrounds stated: *"I am afraid of being hacked because I now do a lot of things and buy a lot of things online,"*.

Financial loss. The adult groups – all groups except for the teenagers – reported more concerns about financial loss compared to teenagers (7%). Older adults had most concerns about financial loss (21%), which might be linked with their transition to retirement and assets to manage at this life stage. In line with prior work [81], older adults' concerns about financial loss were also intertwined with concerns about cybercrime such as scams: e. g., *"Many scammers lurk on the internet and just want to rip off your money."*

Malware and password theft. Compared to the other groups, more teenagers reported concerns about malware (e. g., *"I am concerned about viruses on the mobile phone and on my laptop"*) and password theft (*"I am concerned that my passwords are hacked"*). Participants with migration backgrounds and participants with low education had these concerns to a similar extent, but these concerns were mentioned less frequently by older adults.

Data theft. Participants with migration backgrounds were more concerned about data theft (19%) than the other groups, especially compared to older adults (6%). One participant with migration backgrounds put it this way: *"I'm afraid that my data will be stolen without me knowing or wanting it."* Older adults' lower concern about data theft could also be viewed together with our earlier findings about their relatively low device usage (Section 4.1), which could imply that they had less data "out there."

Phishing. Phishing was mentioned infrequently across all groups (between 4% and 7%), but the few participants that named phishing were aware of its risks and tried to take measures. One participant with low formal education stated: *"In general I am afraid of spear phishing, as I have already been affected by it and I am always very cautious when opening unknown emails."* Contrary to prior measurement studies that shows the prevalence of phishing attacks in the wild [82], [83], [84] our participants seem not that concerned about phishing-related risks.

Tracking and surveillance. While concerns about data collection, aggregation, and use were also relatively low across the groups (between 4% and 6%), participants with migration backgrounds stood out for having slightly higher concerns (9%). This finding could be contextualized in prior work highlighting the pervasive government surveillance they are experiencing [85] and our earlier finding about their higher device usage (see Section 4.1). One participant commented on tracking from for-profit companies, who are also known to exchange data with government agencies [85]: *"You never know how long or where data links are stored . . . at Google Cloud, Whats App chat histories and online purchase service portals and apps . . . They can keep track [of] consumers for a long time."*

Concerns about surveillance were mentioned by more older adults (11%) and participants with low formal education (8%), especially compared to teenagers (1%). These concerns often come with a sense of digital resignation [86], e. g., *"Everything is recorded, you can't hide anything"*.

Table 2. DIGITAL SECURITY CONCERNS (Q4) AMONG OLDER ADULTS, TEENAGERS, PEOPLE WITH MIGRATION BACKGROUNDS, AND PEOPLE WITH LOW FORMAL EDUCATION. THE PERCENTAGES RELATE ONLY TO THOSE PARTICIPANTS THAT REPORT CONCERNS.

Code	Older Adults %	Teenagers %	Migra. Backgr. %	Low Education %
Active attack				
Hacker attack	16	24	19	19
Financial loss	21	7	15	12
Data theft	6	14	19	11
Malware	4	21	7	7
Password theft	1	17	6	5
Phishing	4	7	7	4
Tracking				
Data collection, aggregation, and use	6	4	9	5
Passive attack				
Surveillance	11	1	4	8

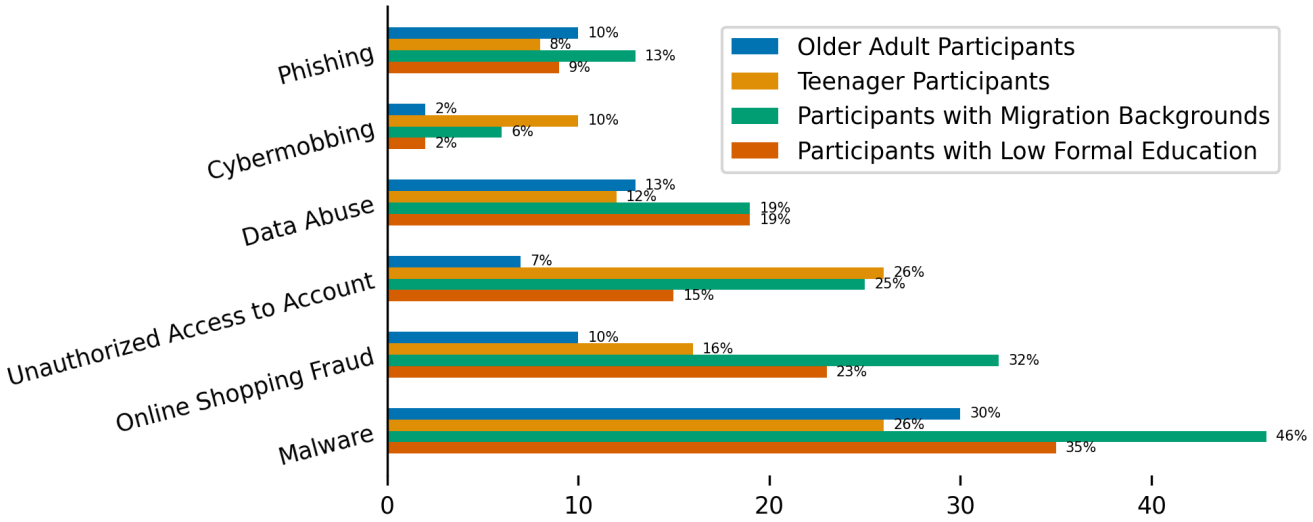

Figure 1. Participants from each group who were affected by different cybercrimes (Q6), rounded to full percentages.

Summary. Participants' concerns about digital security were diverse, and there was no dominant concern across all groups. The primary concern of older adults was about financial loss, whereas teenagers were most concerned about malware. Participants with migration backgrounds had the most concerns about data theft and tracking of all groups.

4.3. Prior Experience with Cybercrime

We asked our participants if they had experienced any of the cybercrime incidents that were part of a German-wide online survey conducted by the BSI with 2000 respondents aged 16-69 [25]. Across all groups, 55% of our participants reported at least one incident – indicating that the prevalence of cybercrime experiences in our sample is much higher than the 29% in the BSI survey. The methodological differences between our work and the BSI survey should be noted when viewing this discrepancy – the BSI survey was administered as a web survey, so participants might be more digitally literate and take more security measures. Our finding also validates the notion that at-risk groups are experiencing more cybercrime than "average" users.

The difference is especially pronounced for participants with migration backgrounds (72% reported experiences with at least one incident). The percentage of prior experience with at least one cybercrime incident is comparatively lower for teenagers and participants with low formal education (both 54%) and for older adults (42%).

Malware. A detailed examination of the specific types of cybercrime incidents (Figure 1) shows that the most common incident was malware – 30% for older adults, 26% for teenagers, 46% for participants with migration

backgrounds, and 35% for participants with low formal education. Those numbers are much higher than in the BSI survey – except for teenagers – in which only 24% reported being affected by malware [25]. Participants with migration backgrounds experienced significantly more malware than teenagers ($X^2 = 19.63, p < 0.05$, $phi = 0.2$) and older adults ($X^2 = 12.65, p < 0.05$, $phi = 0.16$). However, the effect sizes are only small. This finding also contrasts our earlier findings about concerns (Section 4.2), as malware was rarely mentioned as a concern except for teenagers, indicating a misalignment between concerns and actual experiences.

Fraud in online shopping. Our participants' experiences with fraud in online shopping are generally in line with the BSI survey (25%) [25]. 32% of participants with migration backgrounds reported experiencing this – the percentage is significantly higher than that of older adults (10%, $X^2 = 35.92, p < 0.05$) and teenagers (16%, $X^2 = 18.21, p < 0.05$). The difference between older adults (10%) and participants with low formal education (23%) is also significant ($X^2 = 14.48, p < 0.05$). All effect sizes are rather small ($phi < 0.2$). Participants' experiences with fraud in online shopping are reflected in their concerns, as financial loss is a natural consequence of fraud and was mentioned as a concern by participants across the adult groups (Section 4.2).

Unauthorized access to an online account. Teenagers (26%) and participants with migration backgrounds (25%) reported most account compromises (unauthorized access to an online account). Older adults were the least affected (7%), which is not surprising given their comparatively infrequent device usage (Section 4.1). The differences are significant for teenagers versus older adults ($X^2 = 32.22, p < 0.05$, $phi = 0.26$) and teenagers versus participants with low formal education ($X^2 = 8.52, p < 0.05$, $phi = 0.14$). The differences between participants with migration backgrounds and older adults are also significant ($X^2 = 28.89, p < 0.05$, $phi = 0.25$), all with small effect sizes. The higher rate of teenagers being affected is in line with our findings about concerns, as 17% of teenagers reported concerns about password theft which can directly lead to account compromises.

Other cybercrimes. For other less prevalent cybercrime incidents, all groups reported being equally affected by data abuse (percentages between 12% to 19%). The lack of between-group differences also applies to phishing, which was experienced by fewer participants (8% to 13%) and corroborates the limited concerns about phishing in Section 4.2. 10% of teenagers reported experiences with cybermobbing, which is significantly more compared to older adults ($X^2 = 11.86, p < 0.05$, $phi = 0.16$) and participants with low formal education ($X^2 = 13.82, p < 0.05$, $phi = 0.17$), with small effect sizes. For ransomware, cyberstalking, and romance scam, the rates are lower than 5% and similar across all groups; we did not detect any significant between-group differences.

Summary. Our participants encountered more cybercrime incidents compared to the average German population. Participants with migration backgrounds had the most negative incidents (particularly malware and fraud in online shopping), whereas older adults were less affected. Participants' actual experiences with cybercrime are generally in line with their concerns except for malware: teenagers were the most concerned but the least affected, and participants with migration backgrounds encountered significantly more malware than their concerns.

4.4. Potential Attackers

Participants' perceptions of the risks different groups pose to their digital security (Q10) are displayed in Table 3. Participants across all groups rarely perceived people close to them (e. g., family members, friends, and acquaintances) as possible attackers. Interestingly, teenagers identified friends and acquaintances as possible attackers significantly more than the other groups, although the average rating is still "little likely" ($M = 1.74$). The effect sizes were small, except for the post-hoc test for teenagers versus older adults, for which we observed a moderate effect size ($Cohen's\ d = 0.53$). This finding also relates to our earlier finding about how teenagers reported more experiences with cybermobbing in Section 4.3 and echoes past research on a high volume of cybermobbing incidents in school [87].

Similarly, work colleagues were rarely perceived as possible attackers by teenagers, participants with migration backgrounds, and participants with low formal education ($M \approx 2$ for all three groups). Older adults were even less defensive against work colleagues ($M < 1.5$), and the differences between older adults and the other three groups are significant, with small effect sizes ($d < 0.5$).

For officials from Germany (e. g., police, secret services, and the government), participants with migration backgrounds ($M = 2.95$) and participants with low formal education ($M = 2.98$) viewed them as possible attackers significantly more than older adults ($M = 2.68$). The same pattern also applies to officials from other countries and private sector companies. Officials from other countries were viewed significantly less as a risk by teenagers compared to participants with migration backgrounds and low formal education. The effect sizes are small ($d < 0.5$).

By contrast, criminals "who want to get rich from your data" were often identified as possible attackers by many participants. All groups except older adults thought they were "quite likely" to pose risks, whereas older adults only viewed them as moderately risky; the differences between older adults and the other groups are all significant with small effect sizes. We found the same pattern for hackers "who gain unauthorized access to data and devices for fun" as older adults perceived them to be less of a threat than the other groups.

Summary. We do not observe mean values above 4, showing that participants on average did not have high risk perceptions for the possible attackers we queried. Between the different groups, hackers and criminals were viewed as quite a threat, whereas those closer to participants such as family members, friends and acquaintances, and work

Table 3. RATED PROBABILITY (MEAN VALUES) OF EIGHT POSSIBLE ATTACKER GROUPS POSING A RISK TO THE DIGITAL SECURITY OF THE PARTICIPANTS. RATING SCALE RANGING FROM 1–NOT LIKELY TO 5–VERY LIKELY TO POSE RISK.

Group	Possible Attackers							
	Family members	Friends	Work colleagues	Officials from Germany	Officials from other countries	Private sector companies	Criminals	Hackers
Older Adults	1.27	1.31	1.33	1.48	2.68	2.71	3.40	3.13
Teenagers	1.49	1.74	1.54	2.76	2.75	3.00	3.87	3.74
Migra. Backgr.	1.28	1.40	1.67	2.95	3.26	3.22	3.96	3.63
Low Education	1.33	1.47	1.67	2.98	3.26	3.30	4.00	3.60

colleagues were not. Across the four groups, older adults had significantly lower risk perceptions toward these possible attackers than the other groups: the lower risk perceptions could be contextualized in our finding about older adults' lower device usage and prior work on older adults being more trusting than younger adults [88].

4.5. Information Sources

To derive insights on how to best reach different groups for digital security education, we asked participants about their information sources, starting with a binary question on whether they actively seek information about digital security (Q7). Slightly above half of participants with migration backgrounds (54%) reported doing this; the percentage is lower for older adults (41%), participants with low formal education (40%), and teenagers (38%). The differences in information seeking between participants with migration backgrounds and the other groups are all significant, albeit with small effect sizes ($phi < 0.2$). Considering our previous finding that participants with migration backgrounds had disproportionately high encounters with cybercrime incidents, such experiences could serve as strong motivators and learning opportunities [89].

To participants who said they seek information on digital security, we offered a list of possible sources (Q8). The most reported across all groups were friends/family (between 78% and 83%) and online media (between 74% and 84%) (see Figure 2), with no significant between-group differences.

About half of the participants across all groups obtained information from radio or podcasts (between 43% and 51%), again with no significant between-group differences.

Teenagers consult print media much less frequently than other groups, which is also in line with teenagers' tech use patterns in general [90], [91]. The differences are significant for the pairwise comparisons with older adults ($X^2 = 17.44, p < 0.05$, $phi = 0.31$) and with participants with migration backgrounds ($X^2 = 15.57, p < 0.05$, $phi = 0.27$), with small and moderate effect sizes. The same pattern also applies to TV, as teenagers relied on TV as a source of digital security significantly less than older adults ($X^2 = 12.34, p < 0.05$, $phi = 0.26$) and participants with low formal education ($X^2 = 8.50, p < 0.05$, $phi = 0.22$), with small effect sizes ($phi < 0.3$).

In contrast, teenagers used social media significantly more than older adults ($X^2 = 91.20, p < 0.05$, $phi = 0.69$), participants with migration backgrounds ($X^2 = 11.23, p < 0.05$, $phi = 0.23$), and participants with low formal education ($X^2 = 30.31, p < 0.05$, $phi = 0.4$). Older adults use social media much less than the other groups, with also significant differences compared to participants with migration backgrounds ($X^2 = 50.98, p < 0.05$, $phi = 0.47$) and with participants with low formal education ($X^2 = 22.78, p < 0.05$, $phi = 0.35$). Almost all of these effect sizes are moderate ($phi > 0.3$).

Lastly, teenagers also differ from other groups in their use of IT security experts and consumer advice centers/authorities as information sources. Teenagers used security experts significantly less than participants with migration backgrounds ($X^2 = 10.06, p < 0.05$, $phi = 0.22$) and participants with low formal education ($X^2 = 9.97, p < 0.05$, $phi = 0.24$). Teenagers also used consumer advice centers/authorities significantly less than older adults ($X^2 = 9.77, p < 0.05$, $phi = 0.24$).

Summary. While participants reported a variety of information sources, friends/family and online media were used more than others. The reliance on family and peers to navigate digital security threats is also observed in SoKs of at-risk groups [4], [8]. By contrast, our finding differs from Redmiles et al.'s study based on a US national representative sample [92], in which learning from friends/family was not as prevalent as from prompts (such as password meters and update reminders) and automated/forced security (e. g., automatic updates). In terms of between-group differences, we observe that participants with migration backgrounds were the most active information seekers across all groups. Teenagers also exhibited a unique pattern compared to the other three groups as they rely more on social media and rely less on authoritative sources.

5. Discussion

We conducted a large-scale telephone survey with four at-risk groups – older adults, teenagers, people with migration backgrounds, and people with low formal education – using Germany-representative samples. This approach allows us to (1) compare and contrast our findings with prior work (Section 5.1), and (2) systematically and consistently compare the findings about digital security experiences across the four groups, who answered the same questionnaires (Section 5.2). We conclude our paper by discussing how our findings guide future research as well as efforts for security education and policymaking (Section 5.3).

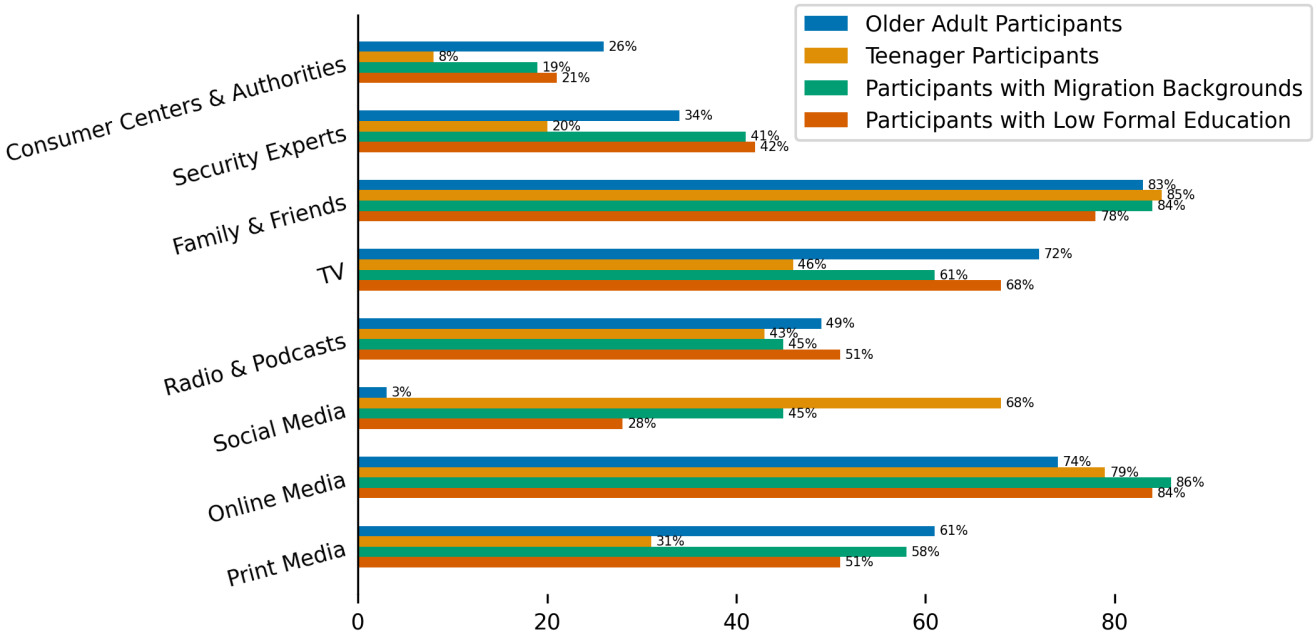

Figure 2. Participants' sources of information (Q8), rounded to full percentages. Only participants who answered "yes" to Q7 are included.

5.1. Comparison With Previous Studies (RQ1)

In this section, we compare and contrast our study's findings with the (predominantly qualitative) prior research on each group presented in Section 2.

5.1.1. Older Adults. Our findings add more nuances to prior work that frames older adults as an at-risk population [8] or highlights the *vulnerability* of older adults to various security and privacy risks [26]. In our study, 42% of our older adult participants reported experiences with cybercrime. While this rate is still much higher than the 29% rate reported in the BSI survey [25], indicating that older adults are at higher risk of experiencing cybercrime than the general population in Germany, their rate is lower than the other three groups. Combined with the finding that older adults use digital devices less frequently, this indicates that older adults may have a smaller attack surface in general.

Regarding information sources, our study revealed similar findings as those from Hornung et al. [27]: participants referred to friends and family for advice on how to protect their data. However, such reliance can introduce new risks when "care surveillance" [93] and insider threats (e. g., financial abuse by a family member) happen.

Nicholson et al. [34] found that older adults value social resources over expert advice for cybersecurity information seeking; our older adult participants exhibited a similar pattern by seeking information from friends and family, but they also used online media, TV, and print media as additional sources, many of which could provide interfaces with experts.

Adding to prior research [26], [81], we provide insights into older adults' digital security concerns, such as financial loss and hacker attacks, and on their risk perception of different groups, which was only negligible to moderate for the queried groups (e. g., for family members or criminals).

5.1.2. Teenagers. Our findings confirm that German teenagers are aware of some of the risks mentioned in Quayyum et al.'s study [21]; hackers, malware, password, and data theft were the most commonly named concerns in our sample. The prevalence we found for teenagers being victimized by cybermobbing or cyberbullying is also in line with findings in related studies [94], [95]. On top of prior work that shows how teenagers engage in a broader variety of online activities than adults [96], including risky behavior such as installing questionable software [97] (which can lead to malware), our findings further highlight the importance of supporting teenagers to cope with malware: our teenage participants not only mentioned malware as a prominent concern but also reported disproportionately high rates of being affected by it.

Our study also provides novel insights into teenagers' information sources for digital security compared to other adult groups. Compared to Redmiles et al. [92], which similarly revealed age-based differences in information but did not look into teenagers in particular, our findings show teenagers' higher reliance on social media and lower reliance on sources from experts and authorities. These findings also relate to the broader literature on teenagers being on the leading edge of the social media space [90].

5.1.3. People with Migration Backgrounds. While many prior studies have focused on specific migration background groups, such as undocumented immigrants and refugees, our research adopts a broader approach by employing the EU definition of migration backgrounds, which includes individuals with at least one parent born in a different country [19]. With the differences in mind, we still compare our findings with these prior studies, as our definition encompasses the aforementioned more specific groups and the comparisons are based on some common grounds. Our participants with migration backgrounds reported high rates of device usage, echoing findings that highlight the importance of ICTs within the migration process particularly for refugees [13], [14], [42], [43], [44], [45], [46], [47], [48]. Our participants – most of whom might have established lives in Germany inferred from their education levels and language proficiency – exhibit a similar pattern in terms of high reliance on digital devices: across all groups, they had the highest adoption rate of smartphones as well as IoT devices such as smart speakers and wearables. They also reported the most experiences with cybercrime, echoing prior work on how this group inevitably bears risks of technology use in exchange for the associated needs and benefits [12], [13].

Similar to Stapf [44], we also found participants with migration backgrounds often asked friends and family for security advice, and relied less on official sources and consumer protection bodies, which is likely a reflection of issues in these sources not meeting their needs (e. g., the materials are hard to understand or require cultural knowledge).

We additionally provide novel insights into this group's most salient security-related concerns – hacker attacks and data theft – and their perception of possible attackers – mainly criminals and not at all family and friends.

5.1.4. People with Low Formal Education. In line with Redmiles et al. [57], our results indicate that we should not assume that lower education is correlated with more exposure to security threats. Redmiles et al. found that people with lower educational attainment report equal or fewer incidents than more educated people [57]; participants with lower education in our study reported more experiences with cybercrime than the average German population, but fewer experiences than some of the more educated groups in our sample. Moreover, contrary to Redmiles et al. [92], we did not find a digital divide in our participants' source selections either, as participants with lower education followed the same pattern as the other two adult groups by relying on online media, friends, and family as their primary sources.

We provide novel insights into this group's digital security concerns, namely hacker attacks and financial loss. Similar to people with migration backgrounds, they identified hackers and criminals as possible attackers more than those in their inner circle.

5.2. Recap of Between-Group Comparisons (RQ2)

Our research joins forces with prior work that synthesizes the disjoint and sometimes contradictory digital security needs of various at-risk groups [4], [8]. Moreover, our research provides novel insights into the ways in which the four at-risk groups we investigated – older adults, teenagers, people with migration backgrounds, and people with low formal education – are similar but also different in their digital security-related concerns and experiences.

5.2.1. All Groups Trust Friends and Family. We found that all four groups were the least concerned about people close to them (e. g., family members, friends and acquaintances, and work colleagues) posing a threat to their digital security. Friends and family were also one of the primary sources our participants used to obtain information about digital security across all groups. These findings suggest our participants' trust in their family and friends when navigating digital security threats, and echo Warford et al. 's SoK [8] that highlights at-risk users' reliance on social connections for advice and support. Nevertheless, such reliance comes with its own risks when people share sensitive digital resources [98] and when groups like older adults are subject to "family surveillance" as their family members become too paternalistic in the efforts to protect them [99].

5.2.2. Hackers Stand Out, Phishing Does Not. All groups universally viewed hackers and criminals as a threat to their digital security, although (surprisingly) only to a rather moderate extent. We can contextualize this finding in our participants' information sources with online media, print media, and TV being the major ones. Additionally, prior work has shown how data breaches are prominently featured in security and privacy news [100] (which can prompt concerns about hackers) and how mass media's portrayal of "hacking" can be inaccurate and exaggerated [101], influencing users' mental models [102].

Interestingly, phishing does not trigger prominent concerns for any of the four groups, despite phishing being a recurring theme in security literature and advice [79], [80] and the prevalence of anti-phishing training programs in research and organizational settings [103], [104], [105]. While experiences with phishing were uncommon in both our study and in the BSI survey [25], our participants reported falling for phishing even less frequently (between 8% and 12%) than respondents to the BSI survey.

Prior work on the demographic differences in phishing susceptibility suggests that women (compared to men) and younger people (18-25 compared to those older) are more susceptible to phishing [106]. Adding to this body of literature, our findings suggest that even though the four groups are characterized as "at-risk," they may not be at higher risk of falling for phishing compared to the general population. However, it is also possible that the phishing rates were under-reported in our study because phishing awareness has not reached the groups when educational efforts are

distributed through the wrong channels. For example, anti-phishing training is mostly deployed in corporate settings, while most older adults and teenagers are not employed. Another possibility is that our participants experienced phishing but were not aware of it or equated phishing with other concepts such as unauthorized access. The differences between our participants' concerns and the actual prevalence of phishing attacks measured in the wild [82], [84] suggest that the four groups might need more education on this threat.

5.2.3. Differences Shaped by Device Usage and Life Stages. Confirming prior work on the "digital divide" of technology use [107], [108], our findings show that older adults are slower adopters across various digital devices, whereas teenagers and participants with migration backgrounds exhibit higher and more diverse device usage. Meanwhile, teenagers and participants with migration backgrounds also reported the most experiences with cybercrime incidents; the rates were also significantly higher than those of older adults across all types of cybercrimes except malware. While we did not conduct correlation analyses to support this, we can already see the intersection between one's device usage and exposure to cybercrimes through these numbers: with more frequent usage of various devices, the possibility of encountering security threats also rises. More device usage also lays the motivation for seeking information on how to secure different devices – this might also explain why participants with migration backgrounds were the most active information seekers across all groups.

Differences in security experiences can also be shaped by one's stage of life. We observe this in multiple comparisons between teenagers and the remaining groups: participants from all adult groups reported more concerns regarding financial loss, while teenagers expressed more concerns regarding malware and password theft. This finding makes sense when contextualizing each group's concerns in their broader life stages. Teenagers tend to have fewer financial resources to manage compared to older adults, whose security and privacy concerns also often center around financial aspects [81]. Financial needs are unlikely to be the primary concern for most teenagers, whereas for people with migration backgrounds, especially refugees, financial needs could become competing priorities that lead them to abandon security best practices [13].

5.3. Implications and Recommendations

Drawing on our findings, we provide education, policy, and future research recommendations for the four at-risk groups we investigated in our study and for research with at-risk user groups in general.

5.3.1. Recommendations for Group-Specific Channels and Content. Our findings on information sources provide insights into the specific channels for reaching each group. For instance, our findings show that teenagers rely on social media for learning about digital security much more than the other groups, indicating that social media (particularly platforms like YouTube, TikTok and Instagram that have high popularity among teenagers [90]) can be used to reach teenagers. On the other hand, television, print media, and sources related to experts and authorities likely work better for older adults who are already using these channels for self-education.

Our findings also provide rich implications on the specific content to be prioritized in designing educational materials for these groups. For instance, for teenagers, the content could focus more on topics that they are less concerned about but report more negative experiences with, such as account compromises and data abuse; attention should also be given to how social media can fuel the learning of anti-security and anti-privacy tactics, such as those for surveilling and controlling others [109]. For people with migration backgrounds and people with low formal education, it is crucial to ensure that the materials are easy to understand, in plain language, while taking into account the potential audience's diverse language skills and cultural backgrounds.

5.3.2. Leverage Social Influence for Security Education. Prior research on social cybersecurity has shed light on how people's security decisions are subject to peer influences [110] and how certain social groups navigate security together [98], [111]. Our findings provide further empirical support for this, as friends and family were among the most utilized sources for learning about digital security across all four groups. Akin to prior work on training cybersecurity guardians in older communities [112], our findings highlight the value of empowering the social circles of at-risk user groups for security education more broadly. More specific pointers can be senior centers and professional caregivers (for older adults); teachers, parents, youth clubs, sports clubs, and influencers on social media (for teenagers), organizations that serve migrants and religious groups (for people with migration backgrounds), organizations that serve people with lower income and local educational personal (for people with low formal education).

Furthermore, there has been a debate on whether to embed mandatory digital security training for children and teenagers at school [113], [114], which, if implemented, can be another source of social influence for this group.

While social influence can be positive, it is worth mentioning how our participants rarely considered people in their inner circles (e. g., friends, family, and work colleagues) as a risk to their digital security. Such trust can be dangerous when one's close social connections become a threat vector, such as in the case of intimate partner abuse [17], elder financial abuse [115], and parental surveillance and control [41], [109]. Educational materials should highlight the possibility of interpersonal adversaries, the corresponding risks, advice on coping strategies, and links to broader resources.

5.3.3. Protect At-Risk Groups through Policymaking. Our findings reveal the four groups are generally more at risk of experiencing security incidents compared to the general German public (see Section 4.3). Thus, these groups

should receive special consideration in laws and regulations that impact one's security, privacy, and digital well-being broadly.

One of our key findings is that participants with migration backgrounds reported the highest device usage, which in turn generates more digital traces [116]; it is then unsurprising to see that they also experienced the most negative security incidents. This inevitable tradeoff this group has to make — exchanging digital security for broader benefits associated with technology use — indicates a failing of society and effective policies that can protect them by default and do not require them to make such tradeoffs. For example, guidance on implementing the GDPR has suggested minors and the elderly as examples of "vulnerable persons" [117], but not necessarily people with migration backgrounds and lower education (despite their frequent encounters with security incidents as our study suggests). On a high level, security and privacy policymaking needs to better incorporate considerations of vulnerability by providing more explicit definitions of vulnerable data subjects as well as expanding the examples of vulnerable persons based on evidence from research [118].

5.3.4. Future Research Directions. Our findings add to the very limited body of literature on the security experiences of people with low formal education. However, more research could be done for a population about which so little is known. Building on our findings, we see opportunities for future research to qualitatively elicit reasons behind their concerns as well as develop and evaluate technologies that support this group's learning and self-protection.

Similarly, while our study provides first-of-its-kind empirical evidence for Warford et al.'s call of "consider at-risk users at scale" [8], we believe that more can be done to shed light on the reasons behind the reported experiences for all groups. It also remains a challenge to quantitatively evaluate and compare the impact of a technology design or educational effort across multiple at-risk populations — another direction that can be pursued by future research. Additionally, the finding that all groups rely on friends and family as information sources with little to no concerns about interpersonal adversaries is worth exploring further. Communicating risks associated with people one knows, trusts, and delegates their digital security is a fundamentally sensitive issue. Future research could look into the specific ways of helping users develop sensible precautions and abilities to watch out for abuse without assuming friends-and-family helpers as a security risk.

6. Conclusion

Our study contributes to the body of research on inclusive security and privacy by examining the digital security experiences of four at-risk groups – older adults, teenagers, people with migration backgrounds, and people with low formal education – through a large-scale (n=1,003) study with demographically representative samples for each group. Since demographically representative samples for these groups can not or not easily be obtained from online panels, we used computer-assisted telephone interviews (CATIs) to investigate participants' device usage, security concerns, prior cybercrime incidents, perceptions of potential attackers, and information sources for security (RQ1), as well as the differences and similarities between the four groups (RQ2). Our results show that participants with low formal education do not have distinctive patterns compared to participants with migration backgrounds, but exhibit significant differences compared to teenagers and older adults. Teenagers and participants with migration backgrounds had higher and more diverse device usage while reporting the most experiences with cybercrime. Conversely, older adults indicated lower device usage, were less affected by cybercrime, and had lower risk perceptions regarding possible attackers. The adult sample groups relied more on traditional information sources, whereas teenagers mainly obtained information about digital security from social media. All groups similarly identified friends and family and online media as their most used information sources and did not regard their social circles as possible attackers. Our research lays the foundation for more cross-group comparisons and syntheses of at-risk users' diverse experiences. Our findings also help identify specific educational approaches, policy recommendations, and directions for future work.

Acknowledgments

We would like to thank Leonie Schaewitz, Carina Wiesen, and Jennifer Friedauer for their support, as well as all participants in our study and our CATI provider. This work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972 and by the federal state of NRW, Germany through the PhD School "SecHuman – Security for Humans in Cyberspace".

References

[1] M. Kaur, M. van Eeten, M. Janssen, K. Borgolte, and T. Fiebig, "Human factors in security research: Lessons learned from 2008-2018," *arXiv preprint arXiv:2103.13287*, 2021.

[2] K. Renaud and L. Coles-Kemp, "Accessible and inclusive cyber security: A nuanced and complex challenge," *SN Computer Science*, vol. 3, no. 5, pp. 1–14, 2022.

[3] L. Fritsch, K. S. Fuglerud, and I. Solheim, "Towards inclusive identity management," *Identity in the Information Society*, vol. 3, pp. 515–538, 2010.

[4] S. Sannon and A. Forte, "Privacy research with marginalized groups: What we know, what's needed, and what's next," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW2, pp. 1–33, 2022.

[5] N. McDonald and A. Forte, "The politics of privacy theories: Moving from norms to vulnerabilities," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–14.

[6] A. M. Walker, Y. Yao, C. Geeng, R. Hoyle, and P. Wisniewski, "Moving beyond'one size fits all' research considerations for working with vulnerable populations," *Interactions*, vol. 26, no. 6, pp. 34–39, 2019.

[7] Y. Wang, "The third wave? inclusive privacy and security," in *Proceedings of the 2017 new security paradigms workshop*, 2017, pp. 122–130.

[8] N. Warford, T. Matthews, K. Yang, O. Akgul, S. Consolvo, P. G. Kelley, N. Malkin, M. L. Mazurek, M. Sleeper, and K. Thomas, "SoK: A framework for unifying at-risk user research," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 2344–2360.

[9] M. K. Scheuerman, S. M. Branham, and F. Hamidi, "Safe spaces and safe places: Unpacking technology-mediated experiences of safety and harm with transgender people," *Proceedings of the ACM on Human-computer Interaction*, vol. 2, no. CSCW, pp. 1–27, 2018.

[10] L. Blackwell, J. Hardy, T. Ammari, T. Veinot, C. Lampe, and S. Schoenebeck, "Lgbt parents and social media: Advocacy, privacy, and disclosure during shifting social movements," in *Proceedings of the 2016 CHI conference on human factors in computing systems*, 2016, pp. 610–622.

[11] A. Lerner, H. Y. He, A. Kawakami, S. C. Zeamer, and R. Hoyle, "Privacy and activism in the transgender community," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–13.

[12] T. Guberek, A. McDonald, S. Simioni, A. H. Mhaidli, K. Toyama, and F. Schaub, "Keeping a low profile? technology, risk and privacy among undocumented immigrants," in *Proceedings of the 2018 CHI conference on human factors in computing systems*, 2018, pp. 1–15.

[13] L. Simko, A. Lerner, S. Ibtasam, F. Roesner, and T. Kohno, "Computer security and privacy for refugees in the united states," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 409–423.

[14] L. Coles-Kemp and R. B. Jensen, "Accessing a new land: Designing for a social conceptualisation of access," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–12.

[15] D. Freed, S. Havron, E. Tseng, A. Gallardo, R. Chatterjee, T. Ristenpart, and N. Dell, "" is my phone hacked?" analyzing clinical computer security interventions with survivors of intimate partner violence," *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, pp. 1–24, 2019.

[16] S. Havron, D. Freed, R. Chatterjee, D. McCoy, N. Dell, and T. Ristenpart, "Clinical computer security for victims of intimate partner violence." in *USENIX Security Symposium*, 2019, pp. 105–122.

[17] J. Slupska and L. M. Tanczer, "Threat modeling intimate partner violence: tech abuse as a cybersecurity challenge in the internet of things," in *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited, 2021.

[18] T. Matthews, K. O'Leary, A. Turner, M. Sleeper, J. P. Woelfer, M. Shelton, C. Manthorne, E. F. Churchill, and S. Consolvo, "Stories from survivors: Privacy & security practices when coping with intimate partner abuse," in *Proceedings of the 2017 CHI conference on human factors in computing systems*, 2017, pp. 2189–2201.

[19] T. European Parliament and the Council of the European Union, "Migration and Home Affairs: Person with a Migratory Background," Jun. 2006, https://home-affairs.ec.europa.eu/pages/glossary/person-migratory-background_en, as of April 13, 2023.

[20] UNESCO Institute for Statistics, "International Standard Classification of Education: ISCED 2011," Dec. 2012, http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf, as of April 13, 2023.

[21] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *International Journal of Child-Computer Interaction*, vol. 30, p. 100343, 2021.

[22] F. B. of Investigation (FBI), "Elder fraud report," 2020.

[23] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples," in *IEEE Symposium on Security and Privacy*, ser. SP '19. San Francisco, California, USA: IEEE, May 2019, pp. 227–244.

[24] J. Tang, E. Birrell, and A. Lerner, "Replication: How Well Do My Results Generalize Now? The External Validity of Online Privacy and Security Surveys," in *Symposium on Usable Privacy and Security*, ser. SOUPS '22. Boston, Massachusetts, USA: USENIX, Aug. 2022, pp. 367–385.

[25] A. Onemichl and C. Bolz, "Digitalbarometer 2022: Bürgerbefragung zur Cyber-Sicherheit [German]," 2022, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2022.html, as of April 13, 2023.

[26] A. Frik, L. Nurgalieva, J. Bernd, J. Lee, F. Schaub, and S. Egelman, "Privacy and security threat models and mitigation strategies of older adults," in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019, pp. 21–40.

[27] D. Hornung, C. Müller, I. Shklovski, T. Jakobi, and V. Wulf, "Navigating relationships and boundaries: Concerns around ict-uptake for elderly people," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017, pp. 7057–7069.

[28] H. Ray, F. Wolf, R. Kuber, and A. J. Aviv, ""woe is me": Examining older adults' perceptions of privacy," in *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, ser. CHI EA '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 1–6.

[29] M. Lüders and P. B. Brandtzæg, "'my children tell me it's so simple': A mixed-methods approach to understand older non-users' perceptions of social networking sites," *New media & society*, vol. 19, no. 2, pp. 181–198, 2017.

[30] A. Quan-Haase and I. Elueze, "Revisiting the privacy paradox: Concerns and protection strategies in the social media experiences of older adults," in *International Conference on Social Media and Society*, 2018, pp. 150–159.

[31] G. Demiris, D. P. Oliver, G. Dickey, M. Skubic, and M. Rantz, "Findings from a participatory evaluation of a smart home application for older adults," *Technology and health care*, vol. 16, no. 2, pp. 111–118, 2008.

[32] L. Boise, K. Wild, N. Mattek, M. Ruhl, H. H. Dodge, and J. Kaye, "Willingness of older adults to share data and privacy concerns after exposure to unobtrusive in-home monitoring," *Gerontechnology*, vol. 11, no. 3, pp. 428–435, 2013.

[33] H. Ray, F. Wolf, R. Kuber, and A. J. Aviv, "Why older adults (don't) use password managers," in *USENIX Security Symposium*, 2021, pp. 73–90, https://www.usenix.org/system/files/sec21-ray.pdf.

[34] J. Nicholson, L. Coventry, and P. Briggs, ""If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults," in *ACM Conference on Human Factors in Computing Systems*, ser. CHI '19. Glasgow, Scotland, United Kingdom: ACM, May 2019, pp. 349:1–349:11.

[35] Y.-Y. Choong, M. Theofanos, K. Renaud, and S. Prior, "Case study: exploring children's password knowledge and practices," in *Proceedings 2019 Workshop on Usable Security (USEC)*, ser. USEC '19. San Diego, CA, USA: Internet Society, Feb. 2019.

[36] Mitchell, Kimberly, J. and Jones, Lisa, M. and Finkelhor, David and Wolak, Janis , "Trends in Unwanted Online Experiences and Sexting : Final Report," 2014, https://scholars.unh.edu/ccrc/49/, as of April 13, 2023.

[37] H. Jia, P. J. Wisniewski, H. Xu, M. B. Rosson, and J. M. Carroll, "Risk-taking as a learning process for shaping teen's online information privacy behaviors," in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 2015, pp. 583–599.

[38] P. Wisniewski, H. Jia, N. Wang, S. Zheng, H. Xu, M. B. Rosson, and J. M. Carroll, "Resilience mitigates the negative effects of adolescent internet addiction and online risk exposure," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 4029–4038.

[39] A. Razi, K. Badillo-Urquiola, and P. J. Wisniewski, "Let's talk about sext: How adolescents seek support and advice about their online sexual experiences," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–13.

[40] P. Wisniewski, H. Xu, M. B. Rosson, and J. M. Carroll, "Parents just don't understand: Why teens don't talk to parents about their online risk experiences," in *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*, 2017, pp. 523–540.

[41] A. K. Ghosh, K. Badillo-Urquiola, M. B. Rosson, H. Xu, J. M. Carroll, and P. J. Wisniewski, "A matter of control or safety? examining parental use of technical monitoring apps on teens' mobile devices," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–14.

[42] S. P. Wyche and R. E. Grinter, ""this is how we do it in my country" a study of computer-mediated family communication among kenyan migrants in the united states," in *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*, 2012, pp. 87–96.

[43] D. Brown, V. Ayo, and R. E. Grinter, "Reflection through design: Immigrant women's self-reflection on managing health and wellness," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014, pp. 1605–1614.

[44] T. Stapf, *Migration/Digital. Die Bedeutung der Sozialen Medien für Ankommen, Orientierung und Teilhabe von Neuzugewanderten in Deutschland [German]*. Berlin: Minor – Projektkontor für Bildung und Forschung, 2019.

[45] N. Kutscher and L.-M. Kress, *Internet ist gleich mit Essen. Empirische Studie zur Nutzung digitaler Medien durch unbegleitete minderjährige Flüchtlinge [German]*. Deutsches Kinderhilfswerk, 2015.

[46] V. Gouma and E. Salto, *Fem.OS – Aufsuchendes Orientierungs- und Beratungssystem in den sozialen Medien für Migrantinnen aus Drittstaaten [German]*. Berlin: Minor – Projektkontor für Bildung und Forschung, 2020.

[47] L. Coles-Kemp, R. B. Jensen, and R. Talhouk, "In a new land: Mobile phones, amplified pressures and reduced capabilities," in *Proceedings of the 2018 chi conference on human factors in computing systems*, 2018, pp. 1–13.

[48] J. Lingel, M. Naaman, and D. M. Boyd, "City, self, network: Transnational migrants and online identity work," in *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, 2014, pp. 1502–1510.

[49] K. B. Sheehan, "Toward a typology of internet users and online privacy concerns," *The information society*, vol. 18, no. 1, pp. 21–32, 2002.

[50] M. Madden, "Privacy, security, and digital inequality," *Data & Society*, 2017.

[51] L. Rainie, S. Kiesler, R. Kang, M. Madden, M. Duggan, S. Brown, and L. Dabbish, "Anonymity, privacy, and security online," *Pew Research Center*, 2013.

[52] D. O'Neil, "Analysis of internet users' level of online privacy concerns," *Social Science Computer Review*, vol. 19, no. 1, pp. 17–31, 2001.

[53] G. R. Milne and M. J. Culnan, "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices," *Journal of interactive marketing*, vol. 18, no. 3, pp. 15–29, 2004.

[54] A. Bergström, "Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses," in *Computers in Human Behavior*, 2015, pp. 419–426.

[55] R. Wash and E. Rader, "Too much knowledge? security beliefs and protective behaviors among united states internet users," in *Symposium on Usable Privacy and Security*, ser. SOUPS '15. Ottawa, Canada: USENIX, Jul. 2015, pp. 309–325.

[56] K. Olmstead and A. Smith, "Americans and cybersecurity," *Pew Research Center*, 2017.

[57] E. M. Redmiles, S. Kross, and M. L. Mazurek, "Where is the digital divide? a survey of security, privacy, and socioeconomics," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ser. CHI '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 931–936. [Online]. Available: https://doi.org/10.1145/3025453.3025673

[58] T. Yan, "Computer-assisted telephone and personal interviews," *The Encyclopedia of Adulthood and Aging*, pp. 1–4, 2015.

[59] I. F. Cervantes and G. Kalton, *Methods for Sampling Rare Populations in Telephone Surveys*. John Wiley & Sons, Ltd, 2007, ch. 5, pp. 113–132.

[60] S. B. (Destatis), "Equipment of households with information and communication technology." [Online]. Available: https://www.destatis.de/EN/Themes/Society-Environment/Income-Consumption-Living-Conditions/Equipment-Consumer-Durables/Tables/liste-equipment-households-information-communication-technology-germany.html#

[61] N. Husted and S. Myers, "Mobile location tracking in metro areas: Malnets and others," in *Proceedings of the 17th ACM Conference on Computer and Communications Security*, ser. CCS '10. New York, NY, USA: Association for Computing Machinery, 2010, p. 85–96. [Online]. Available: https://doi.org/10.1145/1866307.1866318

[62] Y. Michalevsky, A. Schulman, G. A. Veerapandian, D. Boneh, and G. Nakibly, "PowerSpy: Location tracking using mobile device power analysis," in *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C.: USENIX Association, Aug. 2015, pp. 785–800. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/michalevsky

[63] H. Givehchian, N. Bhaskar, E. R. Herrera, H. R. L. Soto, C. Dameff, D. Bharadia, and A. Schulman, "Evaluating physical-layer ble location tracking attacks on mobile devices," in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 1690–1704.

[64] X. Lei, G.-H. Tu, A. X. Liu, C.-Y. Li, and T. Xie, "The insecurity of home digital voice assistants-vulnerabilities, attacks and countermeasures," in *2018 IEEE conference on communications and network security (CNS)*. IEEE, 2018, pp. 1–9.

[65] C. Jackson and A. Orebaugh, "A study of security and privacy issues associated with the amazon echo," *International Journal of Internet of Things and Cyber-Assurance*, vol. 1, no. 1, pp. 91–100, 2018.

[66] A. Zindler and C. Bolz, "Digitalbarometer 2020: Bürgerbefragung zur Cyber-Sicherheit [German]," Sep. 2020, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2020.html, as of April 13, 2023.

[67] M. Callegaro, O. Ayhan, S. Gabler, S. Haeder, and A. Villar, "Combining landline and mobile phone samples: a dual frame approach," *Gesis working paper*, 2011.

[68] L. H. Cox, "A constructive procedure for unbiased controlled rounding," *Journal of the American Statistical Association*, vol. 82, no. 398, pp. 520–524, 1987.

[69] StatistischesBundesamt, "Mikrozensus [german]," https://www-genesis.destatis.de/genesis/online?sequenz=statistikTabellen&selectionname=12211, 2019, [Online; accessed 2022-August-15].

[70] StatistischesBundesamt, "Fortschreibung des bevölkerungsstandes [german]," https://www-genesis.destatis.de/genesis/online?sequenz=statistikTabellen&selectionname=12411, 2020, [Online; accessed 2022-August-15].

[71] J. Cohen, "A power primer." *Methodological issues and strategies in clinical research*, 2016.

[72] P. Mayring, *Qualitative Content Analysis: Theoretical Foundation, Basic Procedures and Software Solution*. Klagenfurt, Austria: SSOAR, 2014.

[73] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice," *Proc. ACM Hum.-Comput. Interact.*, vol. 3, no. CSCW, nov 2019.

[74] C. A. Liang, S. A. Munson, and J. A. Kientz, "Embracing four tensions in human-computer interaction research with marginalized people," *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 28, no. 2, pp. 1–47, 2021.

[75] P. L. Sweet, "Who knows? reflexivity in feminist standpoint theory and bourdieu," *Gender & Society*, vol. 34, no. 6, pp. 922–950, 2020.

[76] U.S. Department of Homeland Security, "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research," Aug. 2012, https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/, as of April 13, 2023.

[77] M. H. Nguyen, J. Gruber, J. Fuchs, W. Marler, A. Hunsaker, and E. Hargittai, "Covid19 changes in digital communication during the covid-19 global pandemic: Implications for digital inequality and future research," *Social Media+ Society*, vol. 6, no. 3, p. 2056305120948255, 2020.

[78] G. Nimrod, "Changes in internet use when coping with stress: older adults during the covid-19 pandemic," *The American journal of geriatric psychiatry*, vol. 28, no. 10, pp. 1020–1024, 2020.

[79] E. M. Redmiles, N. Warford, A. Jayanti, A. Koneru, S. Kross, M. Morales, R. Stevens, and M. L. Mazurek, "A comprehensive quality evaluation of security and privacy advice on the web," in *29th USENIX Security Symposium*. USENIX, 2020, pp. 89–100.

[80] R. W. Reeder, I. Ion, and S. Consolvo, "152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users," *IEEE Security & Privacy*, vol. 15, no. 5, pp. 55–64, Oct. 2017.

[81] A. Quan-Haase and D. Ho, "Online privacy concerns and privacy protection strategies among older adults in east york, canada," *Journal of the Association for Information Science and Technology*, vol. 71, no. 9, pp. 1089–1102, 2020.

[82] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki, D. Margolis, V. Paxson, and E. Bursztein, "Data breaches, phishing, or malware? understanding the risks of stolen credentials," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 1421–1434.

[83] X. Han, N. Kheir, and D. Balzarotti, "Phisheye: Live monitoring of sandboxed phishing kits," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 1402–1413.

[84] APWG, "Phishing Activity Trends Report, 1st Quarter 2022," Jun. 2022, docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf, as of April 13, 2023.

[85] N. Wang, A. McDonald, D. Bateyko, and E. Tucker, "American dragnet: data-driven deportation in the 21st century," *Center on Privacy and Technology at Georgetown Law*, 2022.

[86] N. A. Draper and J. Turow, "The corporate cultivation of digital resignation," *New media & society*, vol. 21, no. 8, pp. 1824–1839, 2019.

[87] S. Alim, "Cyberbullying in the world of teenagers and social media: A literature review." *Breakthroughs in research and practice*, pp. 520–552, 2017.

[88] P. E. Bailey, G. Slessor, M. Rieger, P. G. Rendell, A. A. Moustafa, and T. Ruffman, "Trust and trustworthiness in young and older adults." *Psychology and aging*, vol. 30, no. 4, p. 977, 2015.

[89] Y. Zou, K. Roundy, A. Tamersoy, S. Shintre, J. Roturier, and F. Schaub, "Examining the adoption and abandonment of security, privacy, and identity theft protection practices," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–15.

[90] Vogels, Emily, A. and Gelles-Watnick, Risa and Massarat, Navid, "Teens, Social Media and Technology 2022," Aug. 2022, https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/, as of April 13, 2023.

[91] vom Orde, Heike and Durner, Alexandra, "Grunddaten Jugend und Medien 2023, Aktuelle Ergebnisse zur Mediennutzung von Jugendlichen in Deutschland," 2023, https://izi.br.de/index.htm, as of April 13, 2023.

[92] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How i learned to be secure: a census-representative survey of security advice sources and behavior," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 666–677.

[93] A. Essén, "The two facets of electronic care surveillance: an exploration of the views of older people who live with monitoring devices," *Social science & medicine*, vol. 67, no. 1, pp. 128–136, 2008.

[94] S. Feierabend, T. Plankenhorn, and T. Rathgeb, "JIM 2016 – Jugend, Information, (Multi-) Media [German]," 2016.

[95] H. Möller-Slawinski, "Sinus-Jugendstudie 2021: Cybermobbing im Jugendalltag massiv verbreitet [German]," 2021.

[96] L. Dedkova, D. Smahel, and M. Just, "Digital security in families: The sources of information relate to the active mediation of internet safety and parental internet skills," *Behaviour & Information Technology*, vol. 41, no. 5, pp. 1052–1064, 2022.

[97] S. Furnell, V. Tsaganidi, and A. Phippen, "Security beliefs and barriers for novice internet users," *Computers & Security*, vol. 27, no. 7-8, pp. 235–240, 2008.

[98] H. Watson, E. Moju-Igbene, A. Kumari, and S. Das, ""we hold each other accountable": Unpacking how social groups approach cybersecurity and privacy together," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–12.

[99] S. Murthy, K. S. Bhat, S. Das, and N. Kumar, "Individually vulnerable, collectively safe: The security and privacy practices of households with older adults," *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW1, pp. 1–24, 2021.

[100] S. Das, J. Lo, L. Dabbish, and J. I. Hong, "Breaking! a typology of security and privacy news and how it's shared," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–12.

[101] D. Gordon, "Forty years of movie hacking: considering the potential implications of the popular media representation of computer hackers from 1968 to 2008," *International Journal of Internet Technology and Secured Transactions*, vol. 2, no. 1-2, pp. 59–87, 2010.

[102] K. R. Fulton, R. Gelles, A. McKay, Y. Abdi, R. Roberts, and M. L. Mazurek, "The effect of entertainment media on mental models of computer security," in *Proceedings of the 15th USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2019, pp. 79–95.

[103] R. Wash and M. M. Cooper, "Who provides phishing training? facts, stories, and people like me," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 1–12.

[104] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish," in *Proceedings of the 3rd Symposium on Usable Privacy and Security*, ser. SOUPS '07. New York, NY, USA: Association for Computing Machinery, 2007, p. 88–99.

[105] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching johnny not to fall for phish," *ACM Trans. Internet Technol.*, vol. 10, no. 2, jun 2010.

[106] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2010, pp. 373–382.

[107] Faverio, Michelle, "Share of those 65 and older who are tech users has grown in the past decade," Jan. 2022, https://www.pewresearch.org/fact-tank/2022/01/13/share-of-those-65-and-older-who-are-tech-users-has-grown-in-the-past-decade/, as of April 13, 2023.

[108] O. Huxhold, E. Hees, and N. Webster, "Towards bridging the grey digital divide: changes in internet access and its predictors from 2002 to 2014 in Germany," *European Journal of Ageing*, vol. 17, p. 271–280, 03 2020.

[109] M. Wei, E. Zeng, T. Kohno, and F. Roesner, "Anti-privacy and anti-security advice on tiktok: Case studies of technology-enabled surveillance and control in intimate partner and parent-child relationships," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, 2022, pp. 447–462.

[110] S. Das, T. H.-J. Kim, L. A. Dabbish, and J. I. Hong, "The effect of social influence on security sensitivity," in *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, 2014, pp. 143–157.

[111] Y. Wu, W. K. Edwards, and S. Das, "SoK: Social cybersecurity," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 1863–1879.

[112] J. Nicholson, B. Morrison, M. Dixon, J. Holt, L. Coventry, and J. McGlasson, "Training and embedding cybersecurity guardians in older communities." in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–15.

[113] dpa, "Experten fordern Pflichtfach Informatik in den Schulen," Sep. 2022, https://www.sueddeutsche.de/leben/familie-experten-fordern-pflichtfach-informatik-in-den-schulen-dpa.urn-newsml-dpa-com-20090101-220919-99-820702, as of April 13, 2023.

[114] D. Pencheva, J. Hallett, and A. Rashid, "Bringing cyber to school: Integrating cybersecurity into secondary school education," *IEEE Security & Privacy*, vol. 18, no. 2, pp. 68–74, 2020.

[115] R. Acierno, M. A. Hernandez, A. B. Amstadter, H. S. Resnick, K. Steve, W. Muzzy, and D. G. Kilpatrick, "Prevalence and correlates of emotional, physical, sexual, and financial abuse and potential neglect in the united states: The national elder mistreatment study," *American journal of public health*, vol. 100, no. 2, pp. 292–297, 2010.

[116] S. Shankar, "Coordinating migration: Caring for communities & their data," in *Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing*, 2021, pp. 295–298.

[117] G. University, "GDPR: who are considered to be vulnerable persons?" 2022.

[118] G. Malgieri and J. Niklas, "Vulnerable data subjects," *Computer Law & Security Review*, vol. 37, p. 105415, 2020.

Appendix A. Complete CATI Questionnaire

Demographics

Q_Age: How old are you?

- Items: *14-17; 18-35; 36-50; 51-65; 66-69; 70-79; 80+*

Q_Gender: What is your gender?

- Items: *Female; Male; Non-binary; Describe yourself: [free response]; Prefer not to answer.*

Q_State: In which state do you live?

- Items: *Baden-Württemberg; Bavaria; Berlin; Brandenburg; Bremen; Hamburg; Hesse; Lower Saxony; Mecklenburg-Western Pomerania; North Rhine-Westphalia; Rhineland-Palatinate; Saarland; Saxony; Saxony-Anhalt; Schleswig-Holstein; Thuringia*

Q_Nationality: Were you or at least one part of your parents born with a foreign nationality?

- Items: *Yes; No*

Q_Education: What is your highest level of education?

- Items: *No school leaving certificate; Secondary school (primary school) or equivalent leaving certificate; High school (O level) or equivalent leaving certificate; A level, vocational high school / general or university entrance qualification; Occupational or vocational training / apprenticeship; Completion of a technical college or administrative or professional academy; Bachelor's degree; Diploma university course or masters (including: teaching position, state examination, Master's course, artistic or comparable courses of study); PhD/doctorate; Prefer not to answer.*

Internet Usage

First, I would like to ask you some questions about your internet usage.

Q1 **I'm going to read through a list of devices. Please tell me for each device whether you use it in your daily life or not.** *[multiple choice]*

- Items: *Smartphones; Static PCs / desktop PCs; Laptops; Tablets; Voice assistants or smart speakers (e. g., Alexa, Amazon Echo); Wearables (e. g., fitness trackers or smartwatches)*

Q2 **How often do you use the internet for the following purposes? I'm going to read you a list of purposes and you indicate how often you're using the internet for these purposes.**

- Items: *Online shopping; Ordering services (e.g. booking travel, ordering food); Selling goods or services (e.g. via eBay); Researching information and forming opinions (e.g. reading online newspapers); Uploading and sharing personal content you have created yourself (texts, images, photos, videos) ; Expressing opinions (e.g. posts on social media); Online banking; Communication (e.g. via email and chat); Entertainment (e.g. streaming films, online games); Official transactions (e.g. ordering an identity card); Health services (e.g. electronic patient record, virtual doctor appointment); Map services (e.g. Google Maps or navigation services); Data storage via cloud services*
- Answer Options: *1-Never; 2-Less than once a month; 3-At least once a month; 4-At least once a week, 5-every day; Prefer not to answer.*

Q3 **Next, it's about how you communicate digitally. I'm going to read through a list of communication channels and you tell me in each case how often you use the following communication channels**.

- Items: *Email; Calling via stationary phone; Calling with your smartphone or cell phone; SMS; Messenger services (such as WhatsApp or Signal); Social media (such as Facebook or Instagram); Online forums and communities; Video calls (for example via Skype, Zoom, or Microsoft Teams*
- Answer Options: *Never; Less than once a month; At least once a month; At least once a week, Daily; Prefer not to answer.*

Q4 **Reflecting on the topic of digital security: Is there anything you're concerned about?** Please name anything that comes to your mind spontaneously *[free response]*

Q5 **How familiar are you with the following terms?**

- Items: *Malicious software (for example a computer virus); Ransomware; Phishing; Spear phishing; Two-factor authentication (2FA); Biometric authentication methods; Identity theft; Data leakage or data theft; HTTPS; Hard disk encryption; End-to-end encryption; Transport encryption; Browser; Private browser mode (respectively incognito mode); IP address; URL; Virtual Private Network (VPN); Tor network; ad blocker; Love scam (respectively online love fraud); Spam; Cloud)*
- Answer Options: *I have never heard of this; I have heard about it, but I don't know how it works; I know what it is and how it works; Prefer not to answer.*

Q6 **The next question is about your experiences with cybercrime. Have you been affected to cybercrime yourself? I'm going to read through a list of items and ask you to tell me whether you have ever been affected by them or not.** *[multiple choice]*

- Items: *Malware (such as viruses or Trojans); Phishing, i. e., spying out of confidential data; Ransomware or cryptoviral extortion; Cyberbullying; Online shopping fraud; Foreign access to your online account; Cyberstalking; Victims of data misuse, i. e., the disclosure or sale of personal data (e. g., your telephone number, address, or bank details); Love scam (i. e., love fraud on the internet)*
- Answer Options: *Yes; No; Prefer not to answer.*

Q7 **Do you inform yourself about the topic of *digital security*?**

- *Yes; No*

Q8 *[If "Yes" in Q7]* **The next question is about where you seek information on the topic of digital security. I'll read through the list once again, but related to information sources and you tell me if you're use this respective source to inform yourself on the topic of digital security** *[multiple choice]*

- Items: *Print media; Social media (such as Facebook or Instagram); Radio and/or podcasts; Television; Friends and/or acquaintances and/or family; IT security experts; Consumer advice centers and authorities*
- Answer Options: *Yes; No; Prefer not to answer.*

Q9 You're almost done, there are only a few questions left. **Up next is what data you would like to protect and who you would like to protect your data from. I will read out types of data and ask you to tell me in each case how important it is to you to protect this data on the Internet, for example from outside access and theft.**

- Items: *Your full name; your address or home address; your home telephone number; your contacts; your private photos; message histories (for example, chat and emails); Location and movement histories (for example, GPS data from your jogging route); Amount of salary or earnings; Identification documents (such as, ID card and driver's license); Insurance documents; Delivery bills and invoices; IBAN and BIC, or amount data; Health data; Biometric data (such as fingerprints); Passwords*
- Answer Options: *1-Not important; 2-A little important; 3-Moderately important; 4-Quite-a-bit important; 5-Very important*

Q10 **I'm going to read through a yet another list about groups of people. For each of these groups of people, please tell me how likely you think it is that this group people poses a risk to your digital security – for example, unauthorized access to your personal data, stalk you online or restrict your access to digital services.**

- Items: *Family members; Friends and acquaintances; Work colleagues; Officials from Germany, such as police, secret services and the government; Officials from other countries, such as police, secret services and the government; Private sector companies; Criminals who want to get rich from your data; Hackers who gain unauthorized access to data and devices, for fun.*
- Answer Options: *1-not likely; 2-a little likely; 3-moderately likely; 4-quite a bit likely; 5-very likely.*

Appendix B.
Codebook for Question 4

Table 4. FULL CODEBOOK FOR Q4 ("REFLECTING ON THE TOPIC OF DIGITAL SECURITY: IS THERE ANYTHING YOU ARE CONCERNED ABOUT?") AND ASSIGNMENT FREQUENCIES FOR EACH OF THE FOUR CATI SUBGROUPS (TEENAGERS, OLDER ADULTS, PARTICIPANTS WITH MIGRATION BACKGROUNDS, AND PARTICIPANTS WITH LOW FORMAL EDUCATION).

Code	**CATI**				
	Teenagers $n = 96$	O. Adults $n = 85$	Migration B. $n = 123$	Low Education $n = 123$	Complete $n = 428$
Active Attack					
Unauthorized access to (your) devices	9	2	5	8	24
Financial loss	7	18	19	15	59
Hacker attack	23	14	23	23	83
Data theft (unnoticed)	13	5	23	13	54
Cyberbullying or Cyberstalking	7	-	1	1	9
Fraud	2	7	7	12	28
Malware	20	3	9	9	41
Password theft	16	1	7	6	30
Phishing	7	3	8	5	23
Involuntary publication of personal data	5	-	5	-	10
Fake accounts	1	-	1	2	4
Data misuse	-	2	3	1	6
Criminals	1	2	5	4	12
Identity theft	1	5	8	1	15
Tracking					
Data collection, aggregation, and use	4	5	11	6	26
Unintentional data disclosure	3	2	8	4	17
Profiling	-	-	-	1	1
Cookies	1	1	2	4	8
Personalized advertising	3	4	1	4	12
Forced disclosure of personal data	1	1	2	2	6
Passive Attack					
Eavesdropping	3	2	5	2	12
Data spying	2	3	1	3	9
Lack of data protection	-	3	10	9	22
Surveillance	1	9	5	10	25
General Concerns					
Internet security	2	6	7	10	25
Data loss	3	-	5	1	9
Data protection	7	2	7	5	21
Loss of Control					
Lack of transparency	1	2	2	3	8
Dependency on digital media	-	-	1	1	2
Lack of information (about fraud schemes)	1	1	2	-	4
Life shifts to the virtual world	-	1	-	-	1
No digital forgetting	1	1	-	4	6
Lack of protection and education for children	-	1	3	1	5
Speed of digitalization	1	1	2	-	4
Internet as a lawless space	-	-	-	2	2
Non-targeted Attack		-			
Spam	2	-	1	3	6
No Concerns	4	3	1	4	12
No Codes Possible	8	8	4	8	28

Appendix C.
Meta-Review

C.1. Summary

This papers presents a large-scale analysis of digital security experiences across four at-risk groups in Germany – older adults, teenagers, people with low formal education, and people with a migration background. While all four groups experienced higher rates of cyber misuse compared to previous work on the general German population, some individual variances occurred.

C.2. Scientific Contributions

- Independent Confirmation of Important Results with Limited Prior Research

C.3. Reasons for Acceptance

1) This paper, through phone interviews with 250 people in four separate at-risk groups, provides a large-scale confirmation of previous work on these users. Crucially, it reaches far more participants than is typical for work in this field, which has primarily been limited to small-scale interview studies.
2) This paper situates its results well in comparison to prior literature. While it mostly confirms prior results on a large scale, it also offers nuance to previous findings, especially regarding who these users expect to attack them.

C.4. Noteworthy Concerns

1) Some reviewers were concerned that this paper does not take a sample of a control group for comparison – the paper focuses on between-group comparisons of groups that are at-risk for different reasons.
2) Due to the specific nature of the "migrant" category, comparison with previous work is difficult - the definition of migrant in Germany includes diverse backgrounds and timelines, compared to previous work that is more specific to, e. g., refugees and migrants under specific political pressure. The European Union's definition, which was used by the authors, includes groups from prior work, but also others, like citizens with just one parent born in a different country – this is a broader criterion than most prior work.